WALES AUDIT OFFICE
SWYDDFA ARCHWILIO CYMRU

Date: May 2009

Version 2.1

Information Security Policy

Revision History

Version	Description of changes	Date
V1.0	First version finalised.	February 2006
V1.1	Change of Information Security Officer, amended para 29 such that connection to home broadband network is permitted	October 2007
V2.0	Major revision including more detailed guidance on “care of equipment” and “obtaining business data from clients”.	October 2008
V2.1	Change reflecting that WAO equipment e.g. laptops, memory sticks can be left unattended in vehicles for up to 4 hours if hidden and locked in the boot, or equivalent	May 2009

1 Summary

1. This policy sets out the obligations of all employees arising from the need to control information properly, and the possible consequences if it is not followed – in serious cases, termination of employment.
2. It aims to ensure acceptable use of WAO ICT facilities by outlining the legal requirements for processing data, by defining misuse and by setting out practical security requirements.
3. It highlights key security responsibilities for all staff, including the care and use of usernames and passwords to access information, the care of ICT equipment containing information assets and proper control of the information itself.
4. It also sets out the arrangements that WAO has in place to monitor policy compliance. These include the conditions under which email may be intercepted, the nature of mechanisms that routinely log Internet access and telephone calls, and the monitoring software installed on laptop and desktop machines.
5. It provides contact routes for staff to obtain further support and guidance, and explains how security incidents should be reported.

2 Introduction to Information Security

Purpose and Status of this Document

6. This document sets out the responsibilities of all staff, contract and permanent, regarding the information security policy whilst working within the Wales Audit Office.
7. All staff are required to make themselves familiar with this information security policy, and to confirm that they have read and understood the contents.
8. This document contains the official policy of the organisation. The revision history is shown on the cover sheet.

Statement of Management Intent

9. The Wales Audit Office is committed to maintaining effective security control over the information it receives, stores, manipulates and produces in the course of its duties.
10. Failure to comply with the policy may result in disciplinary action, and in serious cases, termination of employment.

11 Engagement partners (EPs) are responsible to the Chief Operating Officer for information security as it relates to their projects. Each member of staff working as part of a project is responsible to the relevant EP for information security.

Definition of Information Security

12 Information security describes the measures in place:

- To protect information from unauthorised access, modification or disclosure, whether in storage, in processing or during transit, and
- To enable appropriate action to be taken, regarding any such unauthorised events, and to address any underlying issues brought to light.

Objective of the Information Security Policy

13 This information security policy outlines the security procedures and mechanisms, which support and enable the business objectives of the Wales Audit Office whilst properly controlling security risks. These security measures allow information to be safely shared and used.

3 Acceptable Use of Facilities

Lawful use and legal obligations

14 WAO facilities may only be used for lawful purposes. This goes beyond the prohibition of criminal activities; it requires compliance with other legal obligations, such as those of the Data Protection Act 1998. Whilst Annex 1 gives a summary of the main requirements of the Data Protection Act, the WAO's Information Officer should be contacted if further guidance is needed. Contact details are in paragraph 91 of this document.

Misuse

15 Staff must not use WAO facilities in any way that may harm the organisation's reputation. Examples include the unauthorised storage or transmission of material that:

- is obscene or pornographic;
- is likely to cause widespread offence;
- is racist, sexist, malicious, abusive or defamatory in nature;
- constitutes harassment;
- is an infringement of copyright, or is otherwise illegal.

Email – General

16 Email to external organisations is transmitted across the Internet, where it is vulnerable to interception by those with malicious intent. Therefore, external email must not be used to transfer client information which is of "higher sensitivity", as defined in this document in paragraph 55.

17 "Lower sensitivity" information, as defined in paragraph 53, may be sent by email.

18 Provided that the client has given their consent, WAO draft and final reports may be sent by email.

19 Use of the WAO email system to send personal messages is permitted, where the system is available, provided that productivity is not adversely affected. Whilst WAO will use reasonable endeavours to provide an effective email system, however, no responsibility will be taken for personal email which is delivered incorrectly, or which fails to be delivered.

20 Users sending personal emails through the WAO system should mark these as private in the subject line, and / or store them in a similarly-marked email folder. Messages identified thus will not be opened in the course of any monitoring carried out, unless there is a clear reason to do so.

21 The anxiety and disruption caused by "chain letter" circulation of a hoax email warning can be as damaging as a real virus attack. Therefore, users must not use WAO systems to forward or circulate any kind of message which asks readers to forward the message to all of their contacts. Users who are concerned about warnings relating to viruses etc. should forward them only to WAO's Information Security Officer, who will investigate and distribute an advisory note to staff if necessary. Contact details are in paragraph 88 of this document.

(Web) Internet Use

22 Access to Internet websites is filtered, with the aim that websites with inappropriate content, as described in paragraph 15, are made inaccessible. Nonetheless, staff must not attempt to access them. Repeated attempts to access blocked sites will be investigated.

23 Personal use of the Internet is permitted, where available, provided that productivity is not adversely affected.

Laptops and Desktops

24 Laptop or desktop PCs are provided for use by staff, complete with the software needed to support the most common business tasks. Users must not install any kind of software themselves, but should instead contact the

ICT support team for advice, if additional software is needed. Contact details are in paragraph 92 of this document.

25 Staff must not allow any person other than a WAO employee or contractor to have access for any reason to the laptop equipment provided.

Telephones

26 Personal use of desk ‘phones and WAO mobile ‘phones is permitted, provided that productivity is not affected, and costs remain minimal.

Non-WAO Facilities

27 If staff are required to use non-WAO facilities as part of their business duties, for example, those operated by a client body, they should make themselves familiar with, and should adhere to, the policies set out by the client for their use.

4 Staff Responsibilities

Access Control

28 Staff should not divulge any of their passwords to a colleague, or to any member of the ICT Service. Where it is necessary for ICT analysts to log on as the user in order to resolve a support issue, the analyst will reset the password and advise the user of its new value. For their own protection, users should change the password as soon as possible after the support incident has been closed. There is an exception, in that the password for an encrypted memory stick can be shared with a colleague, or member of client staff, in order that the stick can be used to transfer data.

29 Staff must choose a password that is not easily guessable, and must not write the password down.

30 Staff should not log on using a username other than their own.

31 Staff should bear in mind that, where monitoring of computer usage takes place, in most cases the recorded username provides the link to the individual responsible. Staff should therefore take care that they log out, or lock the workstation screen before leaving any session they have logged on.

32 In general, non-WAO PCs must not be connected to the WAO network. However, it may be possible to provide secure Internet access for clients or contractors who bring their own PCs e.g. for a demonstration. Please contact the ICT support team for advice. Contact details are in paragraph 92 of this document.

33 Staff must not seek to circumvent the security controls of WAO, or non-WAO systems in order to gain unauthorised access, and should be aware that the Computer Misuse Act, 1990 made unauthorised access a specific offence, even where no damage is done and no data altered.

Care of Equipment

34 Stakeholders, and the public, have a right to expect that WAO staff will handle information properly. Information stored on laptops, or memory sticks is particularly vulnerable, because of the risk of theft or accidental loss.

35 Whilst WAO has put suitable technical safeguards in place, which protect information through encryption, staff must not rely solely on these. They should still take all reasonable care of WAO equipment in their possession.

36 Staff must not leave equipment unattended in situations where it would be vulnerable to theft. The following paragraphs clarify, through examples, what this means.

37 It is always preferable to remove WAO equipment from a vehicle, before leaving it unattended.

38 However, staff may leave WAO equipment unattended in a vehicle for up to 4 hours at a time. The equipment must be hidden from view and locked in the boot, in a saloon style vehicle. In a hatchback or estate, the equipment must be concealed at the rear using the car's parcel shelf or similar designed for this purpose, and not simply hidden using e.g. a coat.

39 When travelling by train, staff must not leave their laptop or memory sticks unattended. Unless they can be guarded by a colleague, therefore, staff must take these with them when visiting a different part of the train, for example, the buffet car or toilet.

40 In a work environment, staff may leave equipment unattended, for example, at their desk, provided the office has reasonable perimeter security. This means that there is some kind of measure preventing would-be thieves from entering the building – for example, a swipe card system or code lock at the main door, or a turnstile controlled by a manned reception desk.

41 When working in a setting where perimeter security is poor, for example, a hotel suite or client office, where members of the public can walk in unchallenged, staff should either:

i. Ask the client or host to provide a means of locking the room where equipment is to be left, and use this when leaving it unattended, or

ii. Carry the equipment with them at all times.

42 Where staff feel it is appropriate, a steel cable lock can be requested from the ICT support team. Contact details are in paragraph 92 of this document.

43 A cable lock can be used to secure a laptop to a piece of office furniture, such as a table or radiator. This might be useful, for example, when working in a client building which has adequate perimeter security, but where staff, nonetheless, feel the risk of theft is high, perhaps because of the large numbers of unknown staff or contractors present in the building. However, cable locks alone are not adequate to protect equipment in buildings with poor or absent perimeter security, and their use in any event is not mandated.

44 Whilst the security of information entrusted to WAO is very important, the safety of staff is nonetheless paramount. In the event that staff are threatened or attacked by thieves whilst carrying a WAO laptop, it should be surrendered if demanded. Staff must not put themselves at risk.

45 It will be accepted that staff are not at fault, and have taken reasonable care, where equipment is stolen following forced entry to premises (but not to vehicles). Examples include domestic burglary, or theft of a laptop from a locked hotel room or suite. Equally, others may be at fault – for example, where hotel staff erroneously open doors which they should have left locked, leading to theft. Providing staff have acted reasonably – ensuring hotel staff have been asked to keep the doors to a suite locked over lunch, for example – they will not be held responsible in such cases.

46 Theft or loss of WAO equipment, in particular, laptops and memory sticks, resulting from a failure to take reasonable care will be treated as a serious matter, to be dealt with through the disciplinary process.

47 In addition to any disciplinary sanctions, staff may be required to make good the replacement or repair cost of WAO equipment lost or damaged due to their failure to take reasonable care.

48 In any event, loss of equipment should be reported as a security incident to the Information Security Officer (ISO). Contact details are in paragraph 88 of this document.

49 Where the loss is a result of theft or other crime, a crime reference number should be obtained from the Police and provided to the ISO.

50 All equipment must be returned via the line manager when employment finishes, or at the manager's request.

Obtaining Business Data from Clients

51 Obtaining information from clients is a significant source of risk to the organisation if not carried out correctly. Media are easily lost or stolen and, if unencrypted, the contents can be accessed easily by the finder.

52 The following paragraphs differentiate client information into two types, and set out the means by which each of these should be obtained from the client.

Obtaining Business Data of Lower Sensitivity

53 In this document, “lower sensitivity” client information is that which is already in the public domain, or which would readily be provided by the client on request to any person. This includes much routine information handled by clients such as minutes of meetings etc.

54 Lower sensitivity data can be provided by the client to the auditor:

i. by email;

ii. on an encrypted memory stick, which is either exchanged hand to hand, or posted, provided that the password is sent separately, e.g. by text message or email;

iii. on CD or DVD media. If the client is able to use some reasonable means of encrypting the data, this can be posted, otherwise it must be exchanged hand to hand and transferred to the auditor’s laptop whilst on site. If unencrypted, the media must not leave the client site;

iv. in hard copy.

Obtaining Business Data of Higher Sensitivity

55 In this document, “higher sensitivity” client information means all information outside the “lower” category. Higher sensitivity information includes, for example, information about transactions and staff (beyond names in the public domain).

56 Higher sensitivity information, if stored in electronic form, must be provided on an encrypted medium and exchanged hand to hand. It must not be emailed, posted, or placed on unencrypted media.

57 For example, higher sensitivity information could be transferred hand to hand using an encrypted memory stick, or via CD or DVD if the client is able to use some reasonable means of encrypting the data.

58 If there is doubt about the effectiveness of the encryption chosen by the client for use on a CD or DVD, the contents should be transferred to a WAO laptop whilst on site, and the media returned to the client.

59 Encrypted memory sticks containing higher sensitivity information can be removed from the client site, but must not be posted.

60 Once business data of higher sensitivity has been acquired and loaded onto an encrypted memory stick or WAO laptop, it should be transferred onward to a WAO server as soon at the soonest practicable opportunity, and when done, deleted from the memory stick or laptop. The object is to reduce the volume of higher sensitivity data held on laptops and memory

sticks, since the encryption protecting them, whilst strong, cannot be regarded as totally secure.

61 Higher sensitivity information can be transferred hand to hand in hard copy, but hard copy containing such information must never be sent through the post.

62 The WAO's Single Point of Contact (SPOC) within the Compliance team must be informed of all "higher sensitivity" transfers of information between the WAO and clients. Please send an email to SPOC@wao.gov.uk at the outset of each piece of audit work where "higher sensitivity" transfers are needed, explaining briefly the nature of the data required, and the means which will be used to transfer it.

63 The correct procedure for handling of data as part of Computer Automated Audit Techniques (CAATs) which process higher sensitivity data e.g. payroll transactions in bulk, is set out in a separate document, entitled Computer Automated Audit Techniques Procedure. Particular requirements also apply to data matching done to prevent or detect fraud, such as the National Fraud Initiative (NFI). These are set out in the Auditor General's Code of Data Matching Practice http://www.wao.gov.uk/assets/nglishdocuments/Code_of_data_matching_eng.pdf.

Memory Sticks

64 When using encrypted memory sticks to collect information from clients, care must be taken not to expose the client to information inappropriately – for example by passing to the client a stick containing backed up data. If necessary, two sticks should be used, so that a separate device can be used for each of the two purposes - backing up data, and obtaining data from clients.

65 Only the encrypted memory sticks issued by WAO, and no other kind of memory stick, may be connected to WAO computers.

66 Any non-encrypted memory sticks still in users' possession must be handed in to the ICT support team on the 2nd floor, Cathedral Road, to Sandra Fay in Ewloe or Llinos Jones in Swansea/Carmarthen and **not posted**.

Determining Whether the Client Information is Required

67 The need for each element of client data should be considered carefully, particularly if this would fall in the "higher sensitivity" category. Staff must be sure that the risk associated with the transfer of such data is justified, for example, because it is important to the audit work in view, before requesting the data. Personal information (information identifying, or of a significant biographical nature related to, a person) should not be obtained

unless it is strictly necessary for WAO work or other compelling reasons, such as crime prevention.

Personal Computers

68 No client data or working papers of any kind may be transferred by WAO staff to personal computers, unless the data is already in the public domain. This is because personal computers do not have the encryption and other protection mechanisms found on WAO machines.

Backing Up Data

69 Computer hard drives and media (e.g. memory sticks, CD, DVD) are vulnerable to failure without warning.

70 Centralised, automated backup arrangements protect information held on WAO servers, including Outlook mailboxes, network “shared drives”, Sharepoint and the Hub.

71 Individuals are responsible for backing up any data they hold in other locations, including:

i. Outlook messages stored in archives, unless these are stored on network “shared drives”. Each user’s main Outlook mailbox is centrally backed up;

ii. Files held on the laptop C: drive, whether inside or outside of Teammate;

iii. Any files stored on a memory stick, CD or DVD, if they are the only copy.

72 The principle of back up is that an additional copy of each data file is made on a separate medium. If a laptop is then stolen, or its hard disk fails, the work contained on the laptop is not lost, because it can be restored from the back up.

73 Individuals should back up any changed documents daily. By preference, they should do this by copying the changed data to a location which will be automatically backed up, for example, a network “shared drive”. Back up can also be accomplished by uploading a document to Sharepoint, or by emailing it to oneself or a colleague.

74 Where necessary, e.g. because regular access to central systems is difficult, staff can use an encrypted memory stick to back up their laptop data. However, care must then be taken to keep the memory stick separate from the laptop, so that both are not lost at the same time.

75 Some staff may encounter or need to produce documents that are marked in accordance with the UK Government Protective Marking Scheme (GPMS) - for example “Restricted”. These include briefings for the

National Assembly's Audit Committee. For further information, see Annex 2.

Risk Assessment

76 Auditors must undertake regular risk assessments of information security and confidentiality arrangements and consider changes to working practices to safeguard information where appropriate. These may include:

- using unique identifiers to avoid specific reference to personal information;
- requiring all information requests to a client to be made through a single point of contact;
- issuing standard advice to clients on the safe transfer of information with every request for information made;
- amending the Project Initiation Document templates (or their equivalents) to include a section that covers information security and confidentiality;
- reviewing IT options for increasing security of information;
- reviewing, and securely destroying unnecessary information held within files at project closure; and
- including a review of information held as part of quality assurance arrangements.

5 Security Monitoring and Enforcement

Principles for Monitoring

77 The organisation will adhere to the Information Commissioner's Employment Practices Code. Reasonable monitoring procedures will be used by WAO to further an investigation, such as where suspicion of misconduct on the part of a member or group of staff arises from another source, or as set out below.

Email

78 There will be no routine monitoring of the content of employees' email messages, other than through automatic systems designed to reject spam and virus-infected messages.

79 In general, access to staff email accounts will not be provided to line managers, other than with the consent of the individual concerned. Line

managers should therefore ensure that suitable arrangements to access important documents are in place to cover staff leave etc.

Telephone

80 There will be no routine monitoring of the content of employees' telephone calls.

81 Call source and destination numbers, durations, and costs will be analysed periodically to ensure that excessive costs are not incurred.

(Web) Internet Use

82 All Internet web access using WAO facilities will be automatically logged.

83 Access to inappropriate sites will be blocked by a filtering mechanism.

84 Because the filtering technology is not wholly effective, and in view of the reputational risk to WAO, access logs will be scanned periodically for misuse using computer-based, bulk record analysis techniques.

Laptops and Desktops

85 Automatic mechanisms are in place to scan the installed software on laptop and desktop machines and to report this centrally.

86 Document contents will not be routinely scanned or monitored.

6 Contacts for Support and Guidance

Questions on Information Security Policy

87 Questions on WAO's information security policy or the interpretation of this document should be raised with Matthew Jubb, WAO's Head of ICT in the first instance via email, or by 'phone on 02920 320549.

Reporting of Security Incidents

88 Security incidents should be reported to Sarah Hatton, WAO's Information Security Officer (ISO) via email, or by 'phone on 02920 320552. The ISO will co-ordinate the logging of such incidents, and the processes for investigation and resolution, as appropriate.

89 Where security incidents relate to apparent misuse of facilities, the ISO will liaise with HR and line management as appropriate, in order to facilitate the initiation of any required internal investigation, disciplinary procedure or external criminal investigation.

90 Examples of security incidents include:

- Accidental loss of a laptop;
- Unauthorised access to corporate data;
- Intrusion onto WAO premises or theft of equipment.

Data Protection Act 1998, Freedom of Information Act 2000 and other information law requirements

91 If you are unsure of your responsibilities in connection with the Data Protection Act, the Freedom of Information Act and other information law requirements, you should contact Martin Peters, the WAO's Information Officer via email, or by 'phone on 02920 320526.

ICT Support or Advice

92 For support or advice on any general matter relating to ICT, please contact the support team via email to "WAO Support", or by 'phone on 0845 357 0087.

Annex 1 - The Data Protection Act 1998

The eight principles of good practice
Under the Data Protection Act 1998, anyone processing personal information must comply with eight enforceable principles of good information handling practice. These say that data must be:

1. fairly (see the six conditions below) and lawfully processed;
2. processed for limited purposes;
3. adequate, relevant and not excessive;
4. accurate and up to date;
5. not kept longer than necessary;
6. processed in accordance with the individual's rights;
7. secure;
8. not transferred to countries outside European Economic area unless country has adequate protection for the individual.

The six conditions
At least one of the following conditions must be met for personal information to be considered fairly processed:

1. the individual has consented to the processing;
2. processing is necessary for the performance of a contract with the individual;
3. processing is required under a legal obligation (other than one imposed by the contract);
4. processing is necessary to protect the vital interests of the individual;
5. processing is necessary to carry out public functions, e.g. administration of justice;
6. processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could unjustifiably prejudice the interests of the individual).

Sensitive data
Specific provision is made under the Act for processing sensitive personal information. This includes racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health condition, sex life, criminal proceedings or convictions.

For sensitive personal information to be considered fairly processed, at least one of several extra conditions must be met. These include:

- having the explicit consent of the individual;
- being required by law to process the information for employment purposes;
- needing to process the information in order to protect the vital interests of the individual or another person;
- dealing with the administration of justice or legal proceedings.

Annex 2 - Protective Marking

1. Some of the WAO's clients follow the UK Government Protective Marking Scheme (GPMS). The WAO also follows this scheme where it is necessary in order to deal with those audited bodies.
2. Protective marking is a label that indicates the sensitivity of an 'asset', such as a document. The most common of these is "Restricted". The other three labels—"Top Secret", "Secret" and "Confidential"—are unlikely to be relevant to our work.

Definition and examples of "Restricted"

3. Marking is to be determined primarily by reference to the consequences that are likely to result from the 'compromise' of that information, such as its accidental disclosure. "Restricted" assets are defined as such if their compromise would be likely to:

   a) cause substantial distress to individuals;
   b) cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or companies;
   c) prejudice the investigation or facilitate the commission of crime;
   d) breach proper undertakings to maintain the confidence of information provided by third parties;
   e) impede the effective development or operation of government policies;
   f) breach statutory restrictions on the disclosure of information;
   g) disadvantage government in commercial or policy negotiations with others;
   h) undermine the proper management of the public sector and its operations;
   i) adversely affect diplomatic relations;
   j) make it more difficult to maintain the operational effectiveness or security of UK or allied forces.

4. Therefore, in considering whether to mark a document or other asset, one should consider whether compromise would cause one of the above. Examples of documents that should be marked include:

   a) Outline Audit Findings;
   b) Provisional Audit Findings;
   c) Provisional Audit Findings for Finance Director's consideration and comment;
   d) Revised Audit Findings following Finance Director's consideration and comment;
   e) Briefs for Audit Committee Members;
   f) Draft Audit Committee reports;
   g) Draft invitations to tender;
   h) Public interest disclosures;
   i) Documents relating to reporting under the Proceeds of Crime Act and Money Laundering Regulations.

Descriptors

5. Protective marking may be accompanied by descriptors, such as “Appointments”—i.e. concerning actual or potential appointments that have not yet been announced. These additional labels show what sort of sensitive material is being protected and help people handling information to consider what groups of people either should or should not have access to it.

Storage and transmission

6. “Restricted” material should be stored and controlled so as to avoid unauthorised access. Except by specific agreement, it should not be sent by email. For further information, contact “Information Officer” by email.